REMARKS

Claims 1, 2, and 4-32 are pending in the Application. All of those claims stand rejected by the Office Action mailed February 27, 2009. No claims are amended by this response. Claims 1, 11, 15, 21, and 25 are independent claims. Claims 2 and 4-10, 12-14, 16-20, 22-24, and 26-32 depend, respectively, from independent claims 1, 11, 15, 21, and 25.

Applicants respectfully request reconsideration of pending claims 1, 2, and 4-32, in view of the following remarks.

Rejections of Claims

Claims 1-2, 4-7, and 10-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Zhao, United States Patent Application Publication No. 2002/0120124007 (hereinafter "Zhao") in view of Whelan *et al.*, United States Patent Application Publication No. 2004/0203593 (hereinafter "Whelan"). Claims 15-27 and 32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrill *et al.*, United States Patent Application Publication No. 2004/0002943 (hereinafter "Merrill") in view of Whelan. Claims 8-9 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Zhao in view of Whelan, and further in view of Herschberg *et al.*, United States Patent Application Publication No. 2003/0022657 (hereinafter "Herschberg"). Finally, claims 28-31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrill in view of Whelan, further in view of Herschberg.

Applicants respectfully submit that the claims in the Application are allowable for at least the reasons set forth in previous submissions, and those that follow.

I. The Proposed Combination Does Not Render Obvious Claims 1, 2, 4-7, 10-12, And 14

Claims 1-2, 4-7, and 10-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Zhao in view of Whelan. Applicants respectfully traverse those rejections, as discussed more fully below.

Applicants begin with independent claim 1 and its dependent claims. Applicants appreciate the Office Action's recognition that "Zhao fails to teach wherein remote access each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms enabling a particular one of the plurality of server-side components to securely access or manage the at least one associated regions of data and content." (*See* Office Action at p. 3; emphasis in original.) However, the Office Action asserts that Whelan remedies this acknowledged shortcoming in Zhao, stating as follows:

> Whelan et al teaches wherein remote access each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms enabling a particular one of the plurality of server-side components to securely access or manage the at least one associated regions of data and content (See paragraph [0040, 0047, 0048, 0065 and 0085-0087]).

(Office Action at p. 3; emphasis in original.) Applicants respectfully traverse these assertions and submit that Whelan does not teach, suggest, or otherwise render obvious each of a plurality of regions of data and content in the electronic device being controlled by an associated one of a plurality of security mechanisms, let alone wherein remote access to each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms enabling a particular one of the plurality of server-side components to securely access or manage the at least one associated region of the plurality of regions of data and content as claimed. Applicants further note at this time that "the plurality of regions of data and content" as expressly claimed by claim 1 are "in the electronic device." Put another way, claim 1 requires an association between each of the plurality of regions in the

electronic device with one of a plurality of security mechanisms, and that access to a plurality of regions of data and content in an electronic device is controlled by an associated one of a plurality of security mechanisms – in other words, an association of different security mechanisms with different regions of data in the electronic device, with the associated security mechanism controlling access to the associated region of data in the electronic device. As discussed below Whelan does not disclose a plurality of security mechanisms, with one of the security mechanisms associated with each of the regions in the electronic device.

Applicants begin by addressing the first cited portion of Whelan. Paragraph [0040] of Whelan reads as follows:

> [0040] In some embodiments, the one or more configuration management servers may have the capabilities to update software modules and stored data. The configuration management server can determine which versions of software modules and stored data are present on the mobile unit and update versions to the ones specified in the profiles. In most cases, the configuration management server will authenticate the mobile unit and the mobile unit will authenticate the configuration management server before software is updated. This process can involve both update and rollback of versions. Once software or stored data has been updated the installation can be verified to ensure its integrity. The software update procedure can be applied before an association is completed in the case where the mobile unit does not have the correct software or data to operate on a given sub-network. In some embodiments, the configuration management servers can track the licensed software deployed and used on each mobile unit to ensure that license terms and conditions are adhered to.

Applicants respectfully submit that this portion of Whelan merely indicates that a configuration management server and a mobile unit will "authenticate" each other before software is updated. Such a bare reference to authentication of a configuration management server and a mobile device is silent with respect to a plurality of security mechanisms enabling access or management of an associated region of a plurality of regions of data and content in an electronic device. Instead, this portion of Whelan relates to, at most, authentication of an entire mobile unit itself, and does not teach or

suggest anything with respect to association of different security mechanisms with different regions of data in an electronic device. The remaining cited portions of Whelan similarly fail to disclose a plurality of security mechanisms associated with regions of data and content in an electronic device.

For example, the next cited portion of Whelan (Paragraph [0047]) reads as follows:

> [0047] One or more configuration management servers 10 store the profiles 28 for one or more mobile units 18. As a mobile unit roams between the one or more access points 14 on the one or more sub-networks 26, the configuration profile 30 used on the mobile unit is determined by the identity of the access point or sub-network it the mobile unit is associated with. The configuration management client 34 invokes the correct configuration profile and executes it. Periodically, the configuration management client verifies that the required configuration is being maintained. The configuration management server can also distribute software and stored data updates to the mobile units. The one or more sub-networks 26 are connected by one or more backbone networks 24. These networks can be organized in a hierarchy of any required depth. In some deployment situations a network can serve both as a backbone network for other sub-networks and as a sub-network with access points 14. In some embodiments the continuation management server 10 can be distributed between the one or more access points. One or more routers 12, and possibly firewalls, usually interconnect the backbone networks and sub-networks. A configuration management server 10 and security server 20 will provide services to one or more sub-networks. If multiple configuration management servers or multiple security servers are used on one or more of the sub-networks these servers may be arranged in hierarchy to ease the complexity of administration.

This portion of Whelan similarly does not teach or suggest anything with respect to association of different security mechanisms with different regions of data in an electronic device. For example, this portion of Whelan mentions "one or more sub-networks" and "one or more backbone networks," but is entirely silent with respect to a plurality of security mechanisms enabling access or management of an associated

region of a plurality of regions of data and content in an electronic device. Whether or not "multiple security servers are used on one or more of the sub-networks" teaches nothing with respect to different security mechanisms enabling access to different regions of data and content within an electronic device, let alone "wherein remote access to each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms enabling a particular one of the plurality of server-side components to securely access or manage the at least one associated region of the plurality of regions of data and content," as claimed.

The next portion of Whelan relied upon by the Office Action is Paragraph [0048]. That portion of Whelan reads as follows:

> [0048] The one or more security servers 20 authenticate the one or more mobile units 18 associated with the access points 14 on the sub-networks 26. In some embodiments, the mobile unit can authenticate its network connection through the access point using the security server. The security servers typically use a security client 32 on the mobile unit along with stored security information 22 to complete the authentication process. Depending on the implementation, a wide range of authentication schemes may be suitable including, user name and password schemes, symmetric and asymmetric key authentication, and Public Key Infrastructure methods.

This portion of Whelan discusses "one or more security servers" that "authenticate one or more mobile units." Again, to the extent any mobile unit is authenticated in this portion of Whelan, the mobile unit is authenticated as a whole. For example, Whelan states that "the mobile unit can authenticate its network connection through the access point using the security server." Further, "[t]he security servers typically use a security client 32 on the mobile unit along with stored security information 22 to complete the authentication process." Once again, this portion of Whelan discloses, at most, authentication of a mobile unit as a whole, and is utterly silent with respect to a plurality of regions within an electronic device being accessible by different security mechanisms, let alone wherein remote access to each of the plurality of regions

of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms enabling a particular one of the plurality of server-side components to securely access or manage the at least one associated region of the plurality of regions of data and content as claimed. Regardless of whichever of "a wide range of authentication schemes" is employed, the cited portion of Whelan only teaches using any particular scheme for authentication of a mobile unit as a whole, and not the associated plurality of security mechanisms and associated regions of data and content in an electronic device as claimed.

Moving on to the next cited portion, Paragraph [0065] of Whelan reads as follows:

> [0065] The invention provides capabilities for the one or more configuration management servers 10 to propagate changes in data, software or configuration profiles 28, 30 to the mobile units 18. The configuration management client 34 on the mobile unit will periodically poll the server to determine if synchronization is required. Alternatively, when changes to configuration profiles, data or software become available, the configuration management will notify the configuration management client of the pending synchronization. In this case, the server may maintain records used to determine which mobile units need the updates. In either case the server generally verifies that the mobile units are authenticated, possibly using the services of the security server 120, the security information store 22 and the security client 32. The mobile unit may, optionally, authenticate the server or the sub-network 26 association before receiving the software or profile update. The changes are transmitted, th[r]ough the access points 14, to the configuration management clients 34, on the mobile unit, which updates the effected files. Alternatively, if the mobile unit is connected to a wired sub-network 26, via the MU network interface 16, the synchronization occurs th[r]ough this connection. The client and/or the server verify the updates to ensure their integrity. The configuration management server can track the use of licensed software and upgrades. The tracking capabilities can include maintaining records of which mobile unit has each type of licensed software and updating these records when new software or software updates are installed.

Again, Applicants respectfully submit that any discussed authentication of mobile units relates to authentication of a mobile unit as a whole, and does not teach, suggest, or otherwise render obvious the presently claimed subject matter. Further, this portion of Whelan merely mentions an association of a server or sub-network with a mobile device, but is utterly silent with respect to different regions within a device associated with different servers and accessible through different, associated security mechanisms. As such, this portion of Whelan does not remedy the previously discussed shortcomings in the disclosure of Whelan.

Finally, Paragraphs [0085]-[0087] of Whelan read as follows:

> [0085] One or more configuration management servers 400 store the profiles 402 for one or more mobile units 416. As a mobile unit roams between the one or more access points 414 on the one or more sub-networks 412, the configuration profile 402 used for the mobile unit is determined by the identity of the access point or sub-network it the mobile unit is associated with. The configuration management server invokes the correct configuration profile and executes it, typically using the services of the configuration management client 418. For some embodiments, the configuration profile will use a structure nearly identical to the one already described. Periodically, the configuration management server verifies that the required configuration is being maintained. This verification can include testing that configuration parameters are set, that required processes are running, and required connections and sessions are running. As with some other embodiments, the configuration management server can attempt to restore configurations or restart required processes, sessions and connections. If these attempts fail, the mobile unit may be disconnected from the access points or attempt to connect the mobile unit to other access points with different configuration requirements. The configuration management server can also distribute and verify software and stored data updates to the mobile units, much as is done in some other embodiments.
>
> [0086] The one or more sub-networks 412 are connected by a series of one or more backbone networks 410. These networks can be organized in a hierarchy of any required depth. In some deployment situations a network can server

> both as a backbone network for other sub-networks and as a sub-network with access points 414. In some embodiments the continuation management server 400 can be distributed between the one or more access points. One or more routers 408, and possibly firewalls, usually interconnect the backbone networks and sub-networks. A configuration management server 400 and security server 404 will provide services to one or more sub-networks. If multiple configuration management servers or multiple security severs are used on the one or more of the sub-networks these servers may be arraigned in hierarchy to ease the complexity of administration. This hierarchical structure can be nearly identical one already described.
>
> [0087] The one or more security servers 404 authenticate the one or more mobile units associated with the access points 414 on the sub-networks 412. In some embodiments, the mobile unit can authenticate its network connection through the access point using the security server. The security servers typically use a security client 420 on the mobile unit along with stored security information 406 to complete the authentication process. Depending on the implementation, a wide range of authentication schemes may be suitable including, username and password schemes, symmetric and asymmetric key authentication, and Public Key Infrastructure methods.

Again, as also discussed above, whether or not "one or more security servers 404 authenticate the one or more mobile units" is silent with respect to different regions within a device associated with different servers and accessible through different, associated security mechanisms. This portion of Whelan also mentions that "a wide range of authentication schemes may be suitable," but, again, Whelan only teaches, at most, the use of different authentication schemes to authenticate a mobile unit as a whole, and does not teach, suggest, or otherwise render obvious the control of remote access to each of the plurality of regions of data and content in an electronic device by an associated one of a plurality of security mechanisms as claimed. For at least the reasons discussed above, Applicants respectfully submit that the Office Action does not present a *prima facie* case of obviousness for claim 1 and its dependent claims; that the cited art does not teach, suggest, or otherwise render obvious those claims; and that those claims are allowable.

Applicants now turn to independent claim 11 and its dependent claims. Independent claim 11 recites a mobile service network comprising, *inter alia*, "wherein secure access to each of the plurality of associated service components in the electronic device by a corresponding one of the plurality of service management repositories is controlled by an associated one of a plurality of security mechanisms in the electronic device." In asserting that Whelan teaches that aspect of the presently claimed subject matter, the Office Action generally relies on the same aspects of the cited art previously discussed. (*See* Office Action at p. 4.) As such, for at least the reasons discussed above, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness for claim 11 and its dependent claims; that the cited art does not teach, suggest, or otherwise render obvious those claims; and that those claims are allowable.

II. The Proposed Combination Does Not Render Obvious Claims 15-27 And 32

Claims 15-27 and 32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrill in view of Whelan. Applicants begin by addressing the rejection of independent claim 15 and its dependent claims. Claim 15 recites "[a] mobile network for updating firmware and software in an electronic device, the mobile network comprising: a management server facilitating management of firmware and software in the electronic device; a corporate virtual user group management server for corporate virtual user group management; a corporate software repository being employed for corporate virtual user group management and for securely distributing corporate software and corporate data to at least one of a plurality of separate segments of non-volatile memory in the electronic device, the at least one segment associated with a particular user group; and **wherein remote access to each of the plurality of segments of non-volatile memory by the management server is controlled by an associated one of a plurality of security mechanisms in the electronic device**." In asserting that Whelan teaches "wherein remote access to each of the plurality of segments of non-volatile memory by the management server is controlled by an

associated one of a plurality of security mechanisms in the electronic device," the Office Action generally relies on the same aspects of the cited art previously discussed. (*See* Office Action at p. 8.) As such, for at least the reasons discussed above, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness for claim 15 and its dependent claims; that the cited art does not teach, suggest, or otherwise render obvious those claims; and that those claims are allowable.

Turning to independent claim 21, the Office Action asserts that Merrill teaches "wherein remote access to each of the plurality of data segments by a corresponding one of a plurality of data repositories is controlled by an associated one of a plurality of security mechanisms in the electronic device (See paragraph [0064] and [0107])." (*See* Office Action at p. 10; emphasis in original.) Applicants believe that this assertion may be a typographical error, as the Office Action later acknowledges, in connection with claim 25, that "Merrill et al fails to teach wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device." (*See id.* at p. 11; emphasis in original.)

In any event, Paragraph [0064] of Merrill reads as follows:

> [0064] FIG. 5 shows methodological aspects of the framework shown in FIG. 4. Actions on the left-hand side of the figure are performed by components of mobile client device 304. Actions on the right-hand side of the figure are performed by components of management server 302. Actions in the middle are performed by a human being such as by administrator of management server 302 or by a user of the mobile client, the particular of which is specified below in the discussion corresponding to the action. The actions will be described with reference to a scenario where it is desired to distribute and install an application onto a requesting mobile client. An example application has two components: golf.cab and golf.dat. Installation on the mobile device involves copying both components to a directory called "\Program Files\Foo".

Applicants respectfully submit that the above cited portion of Merrill is silent with respect to a plurality of security mechanisms, let alone "wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device" as claimed.

Paragraph [0107] of Merrill reads as follows:

> [0107] In an action 616, download component 414 receives the communicated offering(s) 408 from management server 302. The download component verifies the signature of the download (e.g., a hash) in an action 618, and passes the downloaded files to instruction interpreter 416. In an action 620, the instruction interpreter executes command(s) indicated by an option "command" parameter of the download instruction file 410, which in most cases will initiate installation of the downloaded files by installation component 418. Upon successful installation of an application and/or configuration settings, in an action 622 the user is notified via the notification engine 412 that installation is complete. In one implementation, the server is also notified with a success/failure status message (not shown) of the application delivery and remote configuration actions of the mobile client.

Applicants respectfully submit that this portion of Merrill merely mentions verification of the signature of a download, and does not teach, suggest, or otherwise render obvious a plurality of security mechanisms, let alone "wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device" as claimed. Further, as discussed above, Applicants respectfully submit that the portions of Whelan cited in connection with the rejection of other claims fail to remedy this shortcoming in the teaching of Merrill. As such, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness for claim 21 and its dependent claims; that the cited art does not teach, suggest, or otherwise render obvious those claims; and that those claims are allowable.

Turning to independent claim 25 and its dependent claims, Applicants note that independent claim 25 recites "[a] mobile services network for managing firmware and software in an electronic device, the mobile services network comprising: a plurality of management servers for managing different logical segments of non-volatile memory of the electronic device; the electronic device comprising non-volatile memory segmented into a plurality of logical segments with a different one of the plurality of management servers associated with each of the plurality of logical segments; and **wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device**." In asserting that Whelan teaches "wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device," the Office Action generally relies on the same aspects of the cited art previously discussed. (*See* Office Action at p. 11.) As such, for at least the reasons discussed above, Applicants respectfully submit that the Office Action fails to present a *prima facie* case of obviousness for claim 25 and its dependent claims; that the cited art does not teach, suggest, or otherwise render obvious those claims; and that those claims are allowable.

III. The Proposed Combination Does Not Render Obvious Claims 8 And 9

Claims 8-9 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Zhao in view of Whelan, and further in view of Herschberg. Applicants respectfully submit that claims 8 and 9 depend from independent claim 1. Applicants respectfully submit that Herschberg fails to overcome the above discussed shortcomings in the teachings of Zhao and Whelan. Applicants respectfully submit that because claim 1 is allowable over the proposed combination of references, claims 8 and 9 are also allowable, for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claims 8 and 9 under 35 U.S.C. §103(a) be reconsidered and withdrawn.

IV. The Proposed Combination Does Not Render Obvious Claims 28-31

Claims 28-31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrill in view of Whelan, further in view of Herschberg. Applicants respectfully submit that claims 28-31 depend from independent claim 25. Applicants believe that claim 25 is allowable over the cited combination, in that Herschberg fails to overcome the shortcomings of Merrill and Whelan discussed above. Applicants respectfully submit that because amended claim 25 is allowable over the proposed combination of references, claims 28-31 are also allowable, for at least the same reasons. Accordingly, Applicants respectfully request that the rejection of claims 28-31 under 35 U.S.C. §103(a) be reconsidered and withdrawn.

Conclusion

The Office Action makes various statements regarding the pending claims and the cited references that are now moot in light of the above. Thus, Applicants will not address such statements at the present time. However, Applicants expressly reserve the right to challenge such statements in the future should the need arise (e.g., if such statements should become relevant by appearing in a rejection of any current or future claim).

Applicants believe that all of the pending claims are in condition for allowance. Should the Examiner disagree or have any questions regarding this submission, Applicants invite the Examiner to contact the undersigned at (312) 775-8000 for an interview.

A Notice of Allowability is courteously solicited.

Respectfully submitted,

Date: May 27, 2009

/Kevin E. Borg/
Kevin E. Borg
Reg. No. 51,486

Hewlett-Packard Company
Intellectual Property Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400